IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

HUNTER FREELAND, individually and on behalf of all others similarly situated, Plaintiff, v. NELNET SERVICING, LLC, Defendant.	Case No.: **CLASS ACTION COMPLAINT and JURY TRIAL DEMANDED**

Plaintiff Hunter Freeland ("Plaintiff"), by and through the undersigned counsel, brings this class action complaint against Defendant Nelnet Servicing, LLC ("Nelnet" or "Defendant") on behalf of himself and all others similarly situated. Plaintiff makes the following allegations based upon personal knowledge as to his own actions and upon information and belief as to all other matters.

NATURE OF THE CASE

1. Plaintiff brings this class action against Nelnet for its failure to secure and safeguard student loan borrowers' personally identifiable information ("PII")[1] and for failing to provide timely, accurate, and adequate notice to Plaintiff and Class Members that their PII had been compromised.

2. Nelnet is a Nebraska-based student loan servicing company that also provides technology and web-based services to other student loan servicers. Relevant to this Complaint,

[1] PII is information that is used to confirm an individual's identity, and in this instance includes an individual's name, address, email address, phone number, and Social Security number.

Nelnet provides the student loan servicing systems and customer website portals for Edfinancial Services, LLC ("Edfinancial") and the Oklahoma Student Loan Authority ("OSLA").

3. On August 26, 2022, Nelnet, began notifying state attorneys general and student loan borrowers that it had sustained a massive data breach in which a hacker gained unauthorized access to its networks between June 1 and July 22, 2022 (the "Data Breach").

4. Nelnet admits the hacker accessed highly-sensitive information stored on Nelnet's servers, including student loan borrowers' full names, addresses, email addresses, phone numbers, and Social Security numbers.

5. Nelnet admits that the Data Breach has compromised the PII of over 2.5 million student loan borrowers whose student loans are serviced by Nelnet's customers, Edfinancial and OSLA.

6. Nelnet discovered the unauthorized access on July 21, 2022, but failed to inform the public of the Data Breach until over a month later.

7. The Data Breach occurred because Nelnet negligently failed to implement reasonable security procedures and practices, failed to disclose material facts surrounding its deficient data security protocols, and failed to timely notify the victims of the Data Breach.

8. As a result of Nelnet's failure to protect the sensitive information it was entrusted to safeguard, Plaintiff has already suffered identity theft and fraud and Plaintiff and Class Members also now face a significant risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

PARTIES

9. Defendant Nelnet Servicing, LLC is a Nebraska limited liability company with its principal place of business located at 121 S. 13th Street, Suite 100, Lincoln, Nebraska 68508.

10. Plaintiff Hunter Freeland is a resident of Parkersburg, West Virginia, and a current student loan borrower whose student loans are serviced by Edfinancial. On or about August 28, 2022, Mr. Freeland was notified via letter dated August 26, 2022, that he is a victim of the Data Breach.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists because Nelnet and at least one Class Member are citizens of different States. This Court also has supplemental jurisdiction over the claims in this case pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy under Article III of the United States Constitution.

12. The Court has personal jurisdiction over Nelnet because Nelnet is headquartered in and organized under the laws of Nebraska and is thus essentially at home there. Nelnet also conducts substantial business in Nebraska related to Plaintiff and Class Members and has thereby established minimum contacts with Nebraska sufficient to authorize this Court's exercise of jurisdiction over Nelnet.

13. Venue in the District of Nebraska is proper under 28 U.S.C. § 1391 because Nelnet resides in this District, a substantial part of the conduct giving rise to Plaintiff's claims occurred in this District, and a substantial part of property that is the subject of the action is situated in this District.

FACTUAL ALLEGATIONS

Nelnet's Privacy Practices

14. Nelnet is a student loan servicer that also provides technology and web-based services to other student loan servicers, including, as relevant to this Complaint, Edfinancial and OSLA.

15. Nelnet's parent company, Nelnet, Inc.—incorporated in Nebraska and headquartered in Lincoln—describes itself as having 9,000 associates in 30 communities powering 24 businesses and serving 25 million customers.[2] Nelnet, Inc. has 32 offices in the United States and an office in Australia.[3]

16. In the course of providing technology and web-based services to other student loan servicers, Nelnet collects student loan borrowers' highly sensitive PII, including Social Security numbers. As a result, these student loan borrowers' highly sensitive PII is stored on centralized servers maintained by Nelnet.

17. Nelnet maintains a privacy policy dated August 11, 2021, that is accessible from its website ("Privacy Policy"). Nelnet's Privacy Policy states that "Nelnet takes careful steps to safeguard customer information . . . We maintain reasonable and appropriate physical, electronic, and procedural safeguards to guard your Nonpublic Personal Information (NPI) and Personally Identifiable Information (PII), and we regularly test those safeguards to maintain appropriate levels of protection."[4]

18. On the Privacy Policy frequently asked questions ("FAQ") page of Nelnet's website, Nelnet describes why it collects the personal information of its customers: "We collect

[2] https://nelnetinc.com/ (last visited September 15, 2022)
[3] https://nelnetinc.com/locations/ (last visited September 15, 2022)
[4] https://www.nelnet.com/privacy-and-security (last visited September 15, 2022)

information so we can identify you as our customer, to establish, manage and protect your accounts, to complete your transactions, to create and offer you products and services you might be interested in, to personalize and improve upon your experience with us, and to comply with various legal and regulatory requirements."[5]

19. Nelnet also describes how it collects PII in its Privacy Policy FAQs:

"We may collect Personal Identifying Information (PII) about you from the following sources:

- Information from your loan applications or other loan and account forms
- Information about your transactions with us or others
- Information we receive from third parties, such as your academic institution"[6]

20. On this same page, Nelnet defines PII as "individually identifiable information about an individual customer collected by us and maintained in an accessible form."[7]

21. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Nelnet assumed legal and equitable duties and knew or should have known it was responsible for protecting the PII from unauthorized disclosure.

The Data Breach

22. Between June 1 and July 22, 2022, a hacker infiltrated Nelnet's network and accessed a treasure trove of highly sensitive PII stored on its servers, including full names and Social Security numbers for 2.5 million current or former student loan borrowers.

[5] https://www.nelnet.com/online-policy-faqs (last visited September 15, 2022)
[6] *Id.*
[7] *Id.*

23. Nelnet did not disclose the existence of the Data Breach until over a month later, on August 26, 2022, when it began notifying state attorneys general and affected student loan borrowers.

24. In its notice to state attorneys general, Nelnet vaguely described the Data Breach:

> On or about July 21, 2022, Nelnet Servicing notified Edfinancial and OSLA that it had discovered a vulnerability it believed led to this incident. Nelnet Servicing informed Edfinancial and OSLA that Nelnet Servicing's cybersecurity team took immediate action to secure the information system, block the suspicious activity, fix the issue, and launched an investigation with third-party forensic experts to determine the nature and scope of the activity. On August 17, 2022, this investigation determined that certain student loan account registration information was accessible by an unknown party beginning in June 2022 and ending on July 22, 2022[8]

25. Nelnet's sample form notification letter repeats this description.[9]

26. In September 2022, Nelnet vaguely stated on its website that "On July 21, 2022, Nelnet began notifying impacted student loan servicers that use our servicing system about an isolated incident impacting their website used by borrowers to access account information."[10]

27. Under the website post's section titled "What happened?" Nelnet provides student loan borrowers with no meaningful detail regarding the Data Breach's cause, scope, or impact, downplaying the Data Breach as an "isolated incident impacting [student loan servicers'] website used by borrowers to access account information."[11]

28. Nelnet then admits that its systems contained a vulnerability that needed fixing and that this vulnerability caused the Data Breach: "Our cybersecurity team discovered a vulnerability

[8] https://apps.web.maine.gov/online/aeviewer/ME/40/f6b4d5be-f7ef-412b-9966-e323ad6443a0.shtml (last visited September 15, 2022)
[9] https://oag.ca.gov/system/files/Nelnet%20Servicing%20-%20Sample%20Notice.pdf (last visited September 15, 2022)
[10] https://nelnetinc.com/july-2022-data-security-incident/ (last visited September, 15, 2022)
[11] *Id.*

believed to have led to this incident and took immediate action to secure the systems, block the suspicious activity, and fix the issue."[12]

29. Nelnet further admitted that "[o]n August 17, 2022, the forensics investigation determined that certain student loan account registration information was accessed by an unknown party at times between early June and late July 2022."[13]

30. In contrast to Nelnet's softened description of the Data Breach at the beginning of its website post, under the section titled "Who was affected?" Nelnet admits that its "forensics investigation identified approximately *2.5 million impacted borrowers* whose student loans are serviced by servicers using the affected websites," and under the section titled "What information was involved?" Nelnet admits that "the impacted information included borrowers' name, address, email address, phone number, and Social Security number."[14]

31. Under the section titled "What are we doing?" Nelnet offers empty assurances that "There is no known misuse of information." Nelnet then tacitly admits that victims of the Data Breach are at risk of harm and *places the onus on the data breach victims* by instructing them that "[i]t is important for everyone, not just impacted borrowers, to remain vigilant against identity theft and fraud by regularly reviewing account statements and monitoring free credit reports for any suspicious activity and to detect errors."[15]

32. Nelnet's sample notification letters mimic these same admissions and empty assurances.[16]

---

[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] https://oag.ca.gov/system/files/Nelnet%20Servicing%20-%20Sample%20Notice.pdf (last visited September 15, 2022)

33. Nelnet provides no explanation for why it delayed notifying customers about the Data Breach for almost a month after it detected the Data Breach or why it took Nelnet almost two months to discover the Data Breach. The PII of Plaintiff and Class Members could have been in the hands of hackers for as long as almost three months. By waiting this long to disclose the Data Breach and by downplaying the risk that victims' PII would be misused by bad actors, Nelnet prevented victims from taking meaningful, proactive, and targeted mitigation measures to protect themselves from harm.

34. Nelnet is offering no assistance to Plaintiffs and Class members. Edfinancial and OSLA both state they are offering 24 months of credit monitoring through Experian.

The Data Breach was Preventable

35. In response to the Data Breach, Nelnet stated it "took immediate action to secure the systems, block the suspicious activity, and fix the issue" as soon as it discovered the Data Breach.[17]

36. But Nelnet, like any service provider of its size that stores valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to millions of customer files. Nelnet's implementation of enhanced security measures only after the fact is inexcusable given its knowledge that it was a prime target for cyberattacks.

37. In fact, Nelnet is intimately familiar with data breaches and their devastating impact: in November 2011 a Nelnet employee faced federal criminal charges for unauthorized

[17] https://nelnetinc.com/july-2022-data-security-incident/ (last visited September 15, 2022).

access to Nelnet's servers after the employee stole Nelnet customer information and used it to fraudulently apply for credit cards and loans.[18]

38. Its status as a prime target for cyberattacks was known and obvious to Nelnet as it observed frequent public announcements of data breaches affecting various service providers and understood that the type of information Nelnet collects, maintains, and stores is highly coveted and a frequent target of hackers.

39. Data breaches and the harm they cause have become so common and notorious the Federal Trade Commission ("FTC") has issued guidance for how to address the destruction caused by an unauthorized person having access to someone's PII: "Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[19]

40. At all relevant times, Nelnet knew, or reasonable should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its individual consumers as a result of a breach.

41. Nelnet was, or should have been, fully aware of the significant number of customers whose PII it collected, and thus, the significant number of customers who would be harmed by a breach of its systems.

42. But despite all of the publicly available knowledge of the continued compromises of PII and despite holding the PII of millions of customers, Nelnet failed to use reasonable care in

[18] https://www.databreaches.net/nelnet-employee-accused-of-misusing-customer-info/ (last visited September 15, 2022)
[19] https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf (last accessed September 15, 2022)

maintaining the privacy and security of the PII of Plaintiff and Class Members. Had Nelnet implemented common sense security measures, hackers never could have accessed millions of customer files and the Data Breach would have been prevented or much smaller in scope.

Allegations Relating to Plaintiff Hunter Freeland

43. In approximately 2020, Plaintiff created a student borrower account with his previous student loan servicer in connection with his student loans. In the course of creating his account, Plaintiff had to provide highly sensitive personal information, including, among other things, his Social Security number.

44. In approximately 2021, Plaintiff received notice that his student loan servicer had been changed to Edfinancial.

45. On or about August 26, 2022, Plaintiff received a notification letter from Edfinancial stating that he was a victim of the Data Breach. The letter stated that "Nelnet Servicing, LLC (Nelnet), our servicing system and customer website portal provider, notified us that they had discovered a vulnerability that we believe led to this incident" and that "Nelnet's investigation determined that the impacted information included your name, address, email address, phone number, and Social Security number."

46. The letter recommended that Plaintiff take certain actions like monitoring his accounts and "remain vigilant against incidents of identity theft and fraud over the next 24 months." The letter further asked Plaintiff to "review the information contained in the enclosed '*Steps You Can Take to Help Protect Your Information*.'"

47. Despite making these recommendations, Nelnet also attempted to downplay the risk of harm, stating that "we are not aware of any actual or attempted misuse of your information" and that "[t]his incident did not impact the security of your financial account numbers or payment information." These statements are facially dubious, as the objective of almost every data breach

is to access information that can be misused for financial gain. In any event, Plaintiff would not be able to inform Nelnet of any misuse until *after* the company actually made him aware of the Data Breach.

48. As a result of the Data Breach, Plaintiff has been the victim of extensive identity theft and fraud. On or about August 30, 2022, Amazon notified Plaintiff that they had detected suspicious activity on his account. After checking his Amazon account, Plaintiff discovered an unknown third party had successfully made three fraudulent purchases. Plaintiff had to endure a long and arduous process in attempt to rectify the issue, including spending hours on the phone with Amazon personnel. Ultimately, Plaintiff's Amazon account was closed.

49. Around that same time, Plaintiff's Capital One account was permanently closed due to suspected fraudulent activity. Again, Plaintiff had to devote hours of time on the phone with Capital One personnel addressing the issue. In fact, he only discovered that his Capital One account was closed when his card was declined by a car rental company at the point of sale. At the time, Plaintiff's Capital One card was his only means of payment, and so he had to spend at least 5 hours on the phone at the car rental office trying to figure what happened to his account and out how he was going to pay for the car.

50. On or about August 27, 2022, Plaintiff's PayPal account was locked due to suspicious activity.

51. In late August 2022, Plaintiff's student email account became suddenly and unexpectedly inundated with thousands of spam emails. The spam emails became so crippling that Plaintiff had to spend time communicating with his school in attempt to open a new email account for him that he can actually use.

52. To protect himself from additional harm, Plaintiff has been forced to spend significant time and effort engaging in remedial efforts to protect his information from additional attacks. Plaintiff must now continue to spend time and effort reviewing his financial and other account statements for evidence of unauthorized activity, which he will continue to do indefinitely. Plaintiff suffered significant distress knowing his highly personal information is no longer confidential and his accounts are being targeted.

53. Upon information and belief, Nelnet continues to store and/or share Plaintiff PII on its internal system. Thus, Plaintiff has a continuing interest in ensuring that his PII is protected and safeguarded from future breaches.

Nelnet Failed to Comply with Federal Law and Regulatory Guidance

54. Federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission (FTC) has issued numerous guides for business highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[20]

55. The FTC's publication Protecting Personal Information: A Guide for Business sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[21] Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct

[20] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited September 15, 2022).
[21] *Id.*

security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[22]

56. Additionally, the FTC recommends that organizations limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security; monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[23] This is consistent with guidance provided by the FBI.

57. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[24]

58. Nelnet was fully aware of its obligation to implement and use reasonable measures to protect the PII of its customers but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. Nelnet's failure to employ reasonable measures to protect against unauthorized access to patient information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

59. Defendant also failed to meet the minimum standards of the National Institute of

---

[22] *Id.*
[23] *Id.*
[24] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited September 15, 2022).

Standards and Technology ("NIST") Cybersecurity Framework Version 1.1[25] (including without limitation) PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2).

The Impact of the Data Breach on Victims

60. Nelnet's failure to keep Plaintiff's and Class Members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach—names and Social Security numbers—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class Members now and into the indefinite future. As a result, Plaintiff has suffered injury and faced an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

61. The PII exposed in the Data Breach is highly coveted and valuable on underground markets as it can be used to commit identity theft and fraud. Malicious actors use PII to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can also use consumers' PII to open new financial records, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities." [26]

62. Further, malicious actors often wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be the victims of several cybercrimes stemming from a single data breach.

[25] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last accessed September 15, 2022)

[26] A criminal combines real and fake information to create a new "synthetic" identity, which is used to commit fraud.

63. Victims of the Data Breach face significant harms as the result of the Data Breach, including, but not limited to, identity theft and fraud. Plaintiff and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit monitoring services, reviewing financial and healthcare statements, checking credit reports, and spending time and effort searching for and responding to unauthorized activity.

64. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft; and
- 7% reported feeling suicidal.[27]

65. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate/lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;

[27] https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited September 15, 2022).

- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[28]

66. The unauthorized disclosure of sensitive PII to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm.[29]

67. Consumers are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

68. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. the unconsented disclosure of confidential information to a third party;

b. losing the inherent value of their PII;

c. losing the value of the explicit and implicit promises of data security;

d. identity theft and fraud resulting from the theft of their PII;

e. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

f. anxiety, emotional distress, and loss of privacy;

---

[28] *Id.*

[29] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

g. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

h. unauthorized charges and loss of use of and access to their accounts;

i. lowered credit scores resulting from credit inquiries following fraudulent activities;

j. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

k. the continued, imminent, and certainly impending injury flowing from potential fraud and identify theft posed by their PII being in the possession of one or many unauthorized third parties.

69. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement.

70. There may also be a significant time lag between when personal information is stolen and when it is misused for fraudulent purposes. According to the Government Accountability Office, which conducted a study regarding data breaches: "law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[30]

71. Plaintiff and Class Members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more to work with a provider

[30] http://www.gao.gov/new.items/d07737.pdf (last visited September 15, 2022).

that has better data security. Seventy percent of consumers would provide less personal information to organizations that suffered a data breach.[31]

72. Likewise, the American Bankers Association, reporting on a global consumer survey regarding concerns about privacy and data security, noted that 29% of consumers would avoid using a company that had experienced a data breach, with 63% of consumers indicating they would avoid such a company for a period of time.[32]

73. Plaintiff and Class Members have a direct interest in Nelnet's promises and duties to protect their PII, *i.e.*, that Nelnet *not increase* their risk of identity theft and fraud. Because Nelnet failed to live up to its promises and duties in this respect, Plaintiff and Class Members seek the present value of identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by Nelnet's wrongful conduct. Through this remedy, Plaintiff seeks to restore himself and Class Members as close to the same position as they would have occupied but for Nelnet's wrongful conduct, namely its failure to adequately protect Plaintiff's and Class Members' PII.

74. Plaintiff and Class Members further seek to recover the value of the unauthorized access to their PII permitted through Nelnet's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PII is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the

[31] https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited September 15, 2022).
[32] https://bankingjournal.aba.com/2019/09/what-compliance-needs-to-know-in-the-event-of-a-security-breach/ (last visited September 15, 2022).

reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiff and Class Members have a protectible property interest in their PII; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

75. Nelnet's delayed notice letter also caused Plaintiff and Class Members harm. For example, Nelnet provided no context for its repeated unsubstantiated statement that it was "not aware of any actual or attempted misuse of your information," as the objective of almost every data breach is to gain access to an organization's sensitive data so that the data can be misused for financial gain. Furthermore, the letter did not explain the precise nature of the attack, the identity of the hackers, or the number of individuals affected. Nelnet's decision to withhold these key facts is significant because affected individuals may take different precautions depending on the severity and imminence of the perceived risk. By waiting over a month to disclose the Data Breach and by downplaying the risk of misuse, Nelnet prevented victims from taking meaningful, proactive, and targeted mitigation measures to secure their PII and accounts.

76. Plaintiff and Class Members have an interest in ensuring that their PII is secured and not subject to further theft because Nelnet continues to hold their PII.

CLASS ACTION ALLEGATIONS

77. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> **All individuals residing in the United States whose PII was compromised in the Data Breach.**

78. The Class asserts claims against Nelnet for negligence (Count I), breach of contract (Count II), breach of implied contract (Count III), unjust enrichment (Count IV) and invasion of privacy (Count V).

79. Specifically excluded from the Nationwide Class are Nelnet and its officers, directors, or employees; any entity in which Nelnet has a controlling interest; and any affiliate, legal representative, heir, or assign of Nelnet. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

80. **Ascertainablity.** The members of the Class are readily identifiable and ascertainable. Nelnet and/or its affiliates, among others, possess the information to identify and contact Class Members.

81. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all of them is impracticable. Nelnet's statements reveal that the Class contains more than 2.5 million individuals whose PII was compromised in the Data Breach.

82. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** As to the Class and Subclass, Plaintiff's claims are typical of the claims of the members because all Class Members had their PII compromised in the Data Breach and were harmed as a result.

83. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has no known interest

antagonistic to those of the Class and their interests are aligned with Class Members' interests. Plaintiff was subject to the same Data Breach as Class Members, suffered similar harms, and faces similar threats due to the Data Breach. Plaintiff has also retained competent counsel with significant experience litigating complex class actions, including Data Breach cases.

84. **Commonality and Predominance: Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** There are questions of law and fact common to the Class such that there is a well-defined community of interest in this litigation. These common questions predominate over any questions affecting only individual Class Members. The common questions of law and fact include, without limitation:

a. Whether Nelnet owes Plaintiff and Class Members a duty to implement and maintain reasonable security procedures and practices to protect their PII;

b. Whether Nelnet breached an agreement with Plaintiff and Class Members to keep their PII confidential;

c. Whether Nelnet received a benefit without proper restitution making it unjust for Nelnet to retain the benefit without commensurate compensation;

d. Whether Nelnet acted negligently in connection with the monitoring and/or protection of Plaintiff's and Class Members' PII;

e. Whether Nelnet violated its duty to implement reasonable security systems to protect Plaintiff's and Class Members' PII;

f. Whether Nelnet's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiff and Class Members;

g. Whether Nelnet provided timely notice of the Data Breach to Plaintiff and Class Members; and

h. Whether Plaintiff and Class Members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

85. Nelnet has engaged in a common course of conduct and Plaintiff and Class Members have been similarly impacted by Nelnet's failure to maintain reasonable security

procedures and practices to protect customer's PII, as well as Nelnet's failure to timely alert affected customers to the Data Breach.

86. **Superiority: Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all Class Members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiff knows of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

CLAIMS FOR RELIEF

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

87. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

88. As a condition of having their student loans processed and serviced, Plaintiff and Class Members were required to provide Nelnet and/or its affiliates with their PII. Nelnet collected and stored this PII for purposes of providing services to its customers.

89. Nelnet owed Plaintiff and Class Members a duty to exercise reasonable care in protecting their PII from unauthorized disclosure or access.

90. Nelnet owed a duty of care to Plaintiff and Class Members to provide adequate data security, consistent with industry standards, to ensure that Nelnet's systems and networks adequately protected the PII.

91. Nelnet's duty to use reasonable care in protecting PII arises as a result of the parties' relationship, as well as common law and federal law, and Nelnet's own policies and promises regarding privacy and data security.

92. Section 5 of the Federal Trade Commission Act ("FTC Act") prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Nelnet, of failing to use reasonable measures to protect PII. 15 U.S.C. § 45(a)(1).

93. The FTC publications and orders described above also form part of the basis of Nelnet's duty in this regard.

94. Nelnet violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and failing to comply with applicable industry standards. Nelnet's conduct was unreasonable given the nature and amount of PII they obtained, stored, and disseminated in the regular course of their business, and the foreseeable consequences of a data breach, including, specifically, the significant damage that would result to Plaintiff and Class Members.

95. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

96. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

97. Nelnet's violations of Section 5 of the FTC Act therefore constitute negligence *per se*.

98. Nelnet knew, or should have known, of the risks inherent in collecting and storing PII in a centralized location, Nelnet's vulnerability to network attacks, and the importance of adequate security.

99. Nelnet breached its duty to Plaintiff and Class Members in numerous ways, as described herein, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PII of Plaintiff and Class Members;

b. Failing to comply with industry standard data security measures leading up to the Data Breach;

c. Failing to comply with its own Privacy Policy;

d. Failing to comply with regulations protecting the PII at issue during the period of the Data Breach;

e. Failing to adequately monitor, evaluate, and ensure the security of Nelnet's network and systems;

f. Failing to recognize in a timely manner that PII had been compromised; and

g. Failing to timely and adequately disclose the Data Breach.

100. Plaintiff's and Class Members' PII would not have been compromised but for Nelnet's wrongful and negligent breach of its duties.

101. Nelnet's failure to take proper security measures to protect the sensitive PII of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and exfiltration of PII by unauthorized third parties. Given that financial services providers are prime targets for hackers, Plaintiff and Class Members are part

of a foreseeable, discernible group that was at high risk of having their PII misused or disclosed if not adequately protected by Nelnet.

102. It was also foreseeable that Nelnet's failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiff and Class Members.

103. As a direct and proximate result of Nelnet's conduct, Plaintiff and Class Members have and will suffer damages including: (i) the loss of rental or use value of their PII; (ii) the unconsented disclosure of their PII to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Nelnet's possession and is subject to further unauthorized disclosures so long as Nelnet fails to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; and (ix) any nominal damages that may be awarded.

COUNT II
Breach of Express Contract
(On Behalf of Plaintiff and the Class)

104. Plaintiff repeats and realleges every allegation set forth in paragraphs 1 through 86.

105. Plaintiffs and Class Members were the express, foreseeable, and intended beneficiaries of valid and enforceable contracts between Nelnet and its former and current customers, including Edfinancial and OSLA.

106. Upon information and belief, these contracts include obligations to protect the PII of Plaintiff and Class Members.

107. Upon information and belief, these contracts included promises by Nelnet that expressed or manifested the intent that they were made primarily and directly to benefit Plaintiffs and the Class by protecting their PII, as Nelnet provided services to student loan servicers who own and/or administer the loans of student borrowers including Plaintiff and the Class.

108. Upon information and belief, Nelnet's representations required Nelnet to implement the necessary security measures to safeguard the PII of Plaintiff and the Class.

109. Nelnet failed to implement the necessary measures to safeguard Plaintiff's and Class Members' PII, which was compromised in the Data Breach.

110. The Data Breach was a reasonably foreseeable consequence of Nelnet's actions in breach of these contracts.

111. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure of their PII, the loss of control of their PII, the present risk of suffering additional damages, and out-of-pocket expenses. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

112. Plaintiff repeats and realleges every allegation set forth in paragraphs 1 through 86.

113. Plaintiff and Class Members were required to provide their PII to Nelnet and/or its affiliates in order to have their student loans processed and serviced.

114. As part of these transactions, Nelnet agreed to safeguard and protect the PII of Plaintiff and Class Members. Implicit in these transactions between Nelnet and Class Members was the obligation that Nelnet would use the PII for approved business purposes only and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

115. Additionally, Nelnet implicitly promised to retain this PII only under conditions that kept such information secure and confidential and therefore had a duty to reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or access.

116. Plaintiff and Class Members entered into implied contracts with the reasonable expectation that Nelnet's data security practices and policies were reasonable and consistent with industry standards. Plaintiff and Class Members believed that Nelnet would use part of the monies paid to Nelnet under the implied contracts to fund adequate and reasonable data security practices to protect their PII.

117. Plaintiff and Class Members would not have provided and entrusted their PII to Nelnet or would have paid less for Nelnet's services in the absence of the implied contract between them and Nelnet. The safeguarding of Plaintiff's and Class Members' PII was critical to realizing the intent of the parties.

118. The nature of Nelnet's implied promise itself—the subject matter of the contractual provision at issue—was to protect Plaintiff's and Class Members' PII in order to prevent harm and prevent present and continuing increased risk.

119. Nelnet breached its implied contract with Plaintiff and Class Members by failing to reasonably safeguard and protect their PII, which was compromised as a result of the Data Breach.

120. As a direct and proximate result of Nelnet's breaches, Plaintiff and Class Members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

121. Plaintiff repeats and realleges every allegation set forth in paragraphs 1 through 86.

122. Plaintiff and Class Members have an interest, both equitable and legal, in their PII that was conferred upon, collected by, and maintained by Nelnet and which was stolen in the Data Breach. This information has independent value.

123. Plaintiff and Class Members conferred a monetary benefit on Nelnet in the form of payments for financial services, including those paid indirectly by Plaintiff and Class Members to Nelnet.

124. Nelnet appreciated and had knowledge of the benefits conferred upon it by Plaintiff and Class Members.

125. The price for Nelnet's services that Plaintiff and Class Members paid (directly or indirectly) to Nelnet should have been used by Nelnet, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

126. Likewise, in exchange for receiving Plaintiff's and Class Members' valuable PII, which Nelnet was able to use for their own business purposes and which provided actual value to

Nelnet, Nelnet was obligated to devote sufficient resources to reasonable data privacy and security practices and procedures.

127. As a result of Nelnet's conduct, Plaintiff and Class Members suffered actual damages as described herein. Under principals of equity and good conscience, Nelnet should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds they received as a result of Nelnet's inequitable conduct, including an amount equaling the difference in value between services that included implementation of reasonable data privacy and security practices that Plaintiff and Class Members paid for and the services without reasonable data privacy and security practices that they actually received, and the amount of profit Nelnet made from Plaintiff's and Class Members' accounts while failing to protect their PII.

COUNT V
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

128. Plaintiff repeats and realleges every allegation set forth in paragraphs 1 through 86.

129. Plaintiff and Class Members shared PII with Nelnet and/or its affiliates that Plaintiff and Class Members wanted to remain private and non-public.

130. Plaintiff and Class Members reasonably expected that the PII they shared with Nelnet would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose.

131. Nelnet intentionally intruded into Plaintiff's and Class Members' seclusion by disclosing without permission their PII to a third party who then sold their PII to other third-parties on the dark web.

132. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Nelnet unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, inter alia:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. Invading their privacy by improperly using their PII properly obtained for another purpose, or disclosing it to unauthorized persons;

c. Failing to adequately secure their PII from disclosure to unauthorized persons; and

d. Enabling the disclosures of their PII without consent.

133. The PII that was compromised during the Data Breach was highly sensitive, private, and confidential, as it included Social Security numbers and other information that is the type of sensitive, personal information that one normally expects will be protected from exposure by the entity charged with safeguarding it.

134. Nelnet's intrusions into Plaintiff's and Class Members' seclusion were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

135. As a direct and proximate result of Nelnet's invasion of privacy, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action and appoint Plaintiff and his Counsel to represent the Class;

B. That the Court grant permanent injunctive relief to prohibit and prevent Nelnet from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and Class Members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Nelnet as a result of their unlawful acts, omissions, and practices;

E. That Plaintiff be granted the injunctive relief sought herein;

F. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

G. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial in the instant action.

Dated: September 19, 2022

/s/ *Barrett J. Vahle*
Norman E. Siegel,* Missouri Bar No. #44378
Barrett J. Vahle,* Missouri Bar No. #56674
Benjamin J. Stueve, Missouri Bar No #71197
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
vahle@stuevesiegel.com
ben.stueve@stuevesiegel.com

Cornelius P. Dukelow,* Oklahoma Bar No. 19086
ABINGTON COLE + ELLERY
320 South Boston Avenue, Suite 1130
Tulsa, Oklahoma 74103
(918) 588-3400 (*telephone & facsimile*)
cdukelow@abingtonlaw.com

Christopher P. Welsh, Nebraska Bar No. #22279
WELSH & WELSH PC, LLO
9290 West Dodge Road, Suite 204
Omaha, Nebraska 68114
Telephone: (402) 704-3258
cwelsh@welsh-law.com

**Pro Hac Vice Forthcoming*
Counsel for Plaintiff